Ch 3, Data Analytics: Drawing Conclusions, Part 2

# Data security, 170-175

1. **Why is data security important to an organisation?**

To a business, the loss of data, depending on magnitude, can be anywhere from minor to fatal. Businesses may lose trade secrets to competitors and lose their reputations as trustworthy organisations if they fail to protect their data and information.

1. **Distinguish between deliberate and accidental threats to data.**

Accidental threats are not meant to happen, this can include employee error, power issues or climatic conditions.

Deliberate threats happen purposefully, like hacking or malicious software.

# Physical security

1. **List ways of physically security data.**

* If you use a laptop or tablet and store your data on it, make sure you keep it in a secure place when you are not using it, such as in a cabinet. Otherwise, store it out of sight
* Do not let people you do not know very well use your devices
* If a friend or family member needs to use one of your devices, make sure they cannot access important data
* Keep your doors and windows locked to prevent theft of your hardware
* If you use a desktop computer, keep it switched off when you’re not using it
* Consider using surge-protector power outlets for all your devices to protect the data stored on them

# Software security

1. **Elaborate under each of the following software security strategies:**
   1. **Use strong passwords**

Ideally, passwords should be at least 8 characters in length and include a combination of both uppercase and lowercase letters and numbers. Depending on the software, you may also be able to include special characters such as punctuation.

* 1. **Use login passwords**

You should use login passwords on your laptop, tablet, desktop computer and any other electronic device that has personal or sensitive information on it. You do not want to risk losing it or having it stolen, and having someone else switch it on and have immediate access to everything you have stored on it.

* 1. **Use biometric identification**

While passwords are the only way to control access to remote computers and resources (currently), biometric identification can be used to control computers and resources when the user is physically present. Biometric data cannot be lost, stolen, guessed or discovered easily. Biometric signatures are unique, and include fingerprints, iris patterns (coloured part of eye) and retinal patterns (the blood vessels at the back of the eye).

* 1. **Always log out**

When you are not using a computer any more, do not leave it logged in. Log out and turn-off the monitor. It is easy to forget to log out, but leaving the computer logged in to your user account leaves your data vulnerable to anyone who walks past and sees that the computer is still logged on.

* 1. **Encryption**
     1. **What is public key encryption**

Public key encryption does not need a key to be sent to unlock it.

* + 1. **What is PGP?**

A PGP (pretty good privacy) is software that also uses public key encryption to protect documents.

* 1. **Firewall**

A firewall will prevent unauthorised access to your data and information, and deny networks access to outsiders. Essentially, it will separate the internet and other networks from the computer or LAN on which it is installed. A firewall examines the content of incoming data packets and determines whether they should be allowed to pass through.

* 1. **Antivirus software**
     1. **What is malware?**

Malware is malicious software. It includes viruses, worms, software and Trojan Horses.

* + 1. **What is payload?**

A payload is a term that describes the destructive potential of malware.

* 1. **Backup your files**

Data backups are the final defence against total data loss.